

## CLAIMS

What is claimed is:

- 1 1. A method of preventing an attack on a network, the method comprising the computer-  
2 implemented steps of:  
3 receiving a request to access a resource from a user, wherein the request includes an  
4 accumulated work value;  
5 determining whether the accumulated work value exceeds a required work threshold  
6 value, and if not, selectively requiring the user to perform a quantity of work  
7 as a condition for accessing the resource;  
8 providing the user with access to the resource;  
9 determining an amount of accumulated work output value to provide to the user based  
10 on a volume of data communicated between the resource and the user; and  
11 providing the accumulated work output value to the user.
- 1 2. A method as recited in Claim 1, wherein the request includes a prior user identity  
2 value and a current user identity value, and further comprising the steps of determining  
3 whether a mathematical relationship of the current user identity value and the prior user  
4 identity value indicates that the user has possession of a resource secret.
- 1 3. A method as recited in Claim 1, further comprising the steps of:  
2 receiving a prior keyless user identity value  $H(i+1,x)$  in the request comprising a one-  
3 time password, wherein  $H(i+1,x)$  is computed by the user as a hash chain from  
4 a non-shared user secret ( $x$ ), wherein  $H(n,x) = h(H(n-1,x))$ , wherein  $n > 0$  and  
5  $H(0,x) = x$ , wherein function  $h$  is a one-way function that is difficult to invert;  
6 receiving a current user identity value  $H(i,x)$ ;  
7 verifying that the keyless user identity value properly identifies the user only upon  
8 determining that  $h(H(i,x)) = H(i+1,x)$ .
- 1 4. A method as recited in Claim 3, wherein  $h$  comprises a SHA-1 hash algorithm.

1 5. A method as recited in Claim 3, wherein  $n$  is approximately  $10^4$ .

1 6. A method as recited in Claim 1, further comprising the step of determining the  
2 required work threshold value based on a then-current capacity of the resource.

1 7. A method as recited in Claim 1, further comprising the steps of:  
2 determining the required work threshold value based on a then-current capacity of the  
3 resource;  
4 requiring a first user who has an accumulated work value that is greater than the  
5 required work threshold value to perform a first amount of work as a  
6 condition for accessing the resource; and  
7 requiring a second user who has an accumulated work value that is less than or equal  
8 to the required work threshold value to perform a second amount of work as a  
9 condition for accessing the resource, wherein the second amount of work is  
10 greater than the first amount of work.

1 8. A method as recited in Claim 1, wherein the step of determining an amount of  
2 accumulated work output value is performed for a specified user only during a specified time  
3 period in which accumulating work is allowed for that specified user.

1 9. A method as recited in Claim 1, wherein the step of determining an amount of  
2 accumulated work output value is performed for a specified user only if the current user  
3 identity value received from the user is not found in a list of user identity values that were  
4 previously received in a specified time period.

1 10. A method as recited in Claim 1, further comprising the step of digitally signing and  
2 providing a timestamp to the user with the accumulated work output value, and wherein the  
3 step of determining an amount of accumulated work output value is performed for a specified  
4 user only upon:  
5 receiving the timestamp is received in a subsequent request;

6        verifying the timestamp value; and  
7        determining that the timestamp value is within an allowed range.

1    11.    A method as recited in Claim 1, further comprising the step of receiving the  
2    accumulated proof of work value, a prior user identity value and a current user identity value  
3    in a cookie provided by the user to the resource.

1    12.    A method as recited in Claim 1, wherein determining an amount of accumulated work  
2    output value to provide to the user based on a volume of data communicated between the  
3    resource and the user comprises determining the amount of accumulated work as  $2^k * p$ ,  
4    where k is a number of bits of work previously performed by the user and p is a number of  
5    messages or packets communicated between the user and the resource.

1    13.    A method as recited in Claim 1, further comprising the step of providing the  
2    accumulated work output value in a cookie sent from the resource to the user.

1    14.    A method as recited in Claim 1, further comprising the step of selectively increasing  
2    the required work threshold value for a particular user in response to congestion conditions of  
3    the resource.

1    15.    A method as recited in Claim 1, wherein requiring the user to perform a quantity of  
2    work as a condition for accessing the resource comprises requiring the user to hash a  
3    message until a specified number of bits are zero.

1    16.    A method of preventing an attack on a network, the method comprising the computer-  
2    implemented steps of:

3        receiving a request to access a resource from a user, wherein the request includes an  
4        accumulated work value that represents work that the resource has previously  
5        required the user to perform in order to obtain previous access to the resource;  
6        determining whether the accumulated work value exceeds a required work threshold  
7        value; and

8 providing the user with access to the resource only when the accumulated work value  
9 exceeds a required work threshold value.

1 17. An apparatus for preventing an attack on a network, comprising means for  
2 performing any of the functions recited in any of the steps of Claims 1, 2, 3, 4, 5, 6, 7, 8, 9,  
3 10, 11, 12, 13, 14, 15, or 16.

1 18. An apparatus for preventing an attack on a network, comprising:  
2 a processor;  
3 one or more stored sequences of instructions that are accessible to the processor and  
4 which, when executed by the processor, cause the processor to carry out the  
5 steps of any of Claims 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, or 16.

1 19. A computer-readable medium carrying one or more sequences of instructions for  
2 preventing an attack on a network, wherein execution of the one or more sequences of  
3 instructions by one or more processors causes the one or more processors to perform the  
4 steps of any of Claims 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, or 16.